PATENT ABSTRACTS OF JAPAN

(11)Publication number : 03-239033
(43)Date of publication of application : 24.10.1991

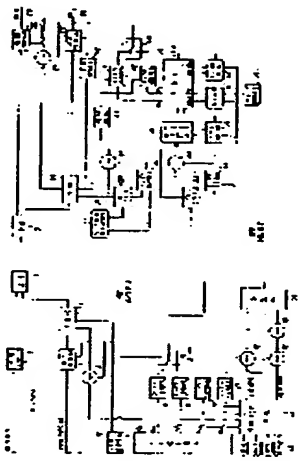
(51)Int.Cl. H04K 1/00
H04N 7/167

(21)Application number : 02-035724
(22)Date of filing : 16.02.1990

(71)Applicant : SONY CORP
(72)Inventor : HOSHINO TAKANARI
YAMASHITA MASAMI
OSADA YASUO

(54) SCRAMBLE SYSTEM AND RECEIVER FOR SCRAMBLE SIGNAL

(57)Abstract:
PURPOSE: To prevent interception by sending an identification signal for a data used for scrambling and for plural data so as to decode all of them.
CONSTITUTION: The changeover of a switch 11 is controlled by a signal from a switching signal generating circuit 12 and a flag (identification signal) representing the switching state is fed to a multiplexer circuit 6. Scrambling using a key signal K1 is applied to a common information signal string and scrambling by using key signals K1, K2 is implemented to an individual information signal string. Thus, a random signal by key signals K3, K4 at the sender side is switched to apply scrambling and a flag (identification signal) representing the switching is sent together with the key signals K3, K4 or the like. On the other hand, the key signals, K3, K4 are detected at the receiver side and a random signal is generated and the flag representing the switching is detected and the random signals are selected to apply signal descrambling.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

decision of rejection]
[Date of extinction of right]

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平3−239033

⑤1Int. Cl.⁵	識別記号	庁内整理番号	⑬公開　平成3年(1991)10月24日
H 04 K 1/00	Z	6914−5K	
H 04 N 7/167		8943−5C	

審査請求　未請求　請求項の数 3　(全7頁)

⑤4発明の名称　スクランブル方式及びスクランブル信号の受信装置

⑳特　願　平2−35724
㉒出　願　平2(1990)2月16日

⑦2発明者　星野　隆也　東京都品川区北品川6丁目7番35号　ソニー株式会社内
⑦2発明者　山下　雅美　東京都品川区北品川6丁目7番35号　ソニー株式会社内
⑦2発明者　長田　保夫　東京都品川区北品川6丁目7番35号　ソニー株式会社内
⑦1出願人　ソニー株式会社　東京都品川区北品川6丁目7番35号
⑦4代理人　弁理士　松隈　秀盛

明　細　書

発明の名称　スクランブル方式及びスクランブル信号の受信装置

特許請求の範囲

1. 第1及び第2のデータのいずれか一方に基づいてスクランブルされた信号と、
上記第1及び第2のデータと、
上記スクランブルされた信号が上記第1及び第2のデータのいずれに基づいているかを示す識別信号とを送付するようにしたスクランブル方式。

2. 第1及び第2のデータが交互に伝送され、かつ伝送される毎にそれぞれ異なる値とされた上記特許請求の範囲第1項記載のスクランブル方式。

3. 上記特許請求の範囲第1項記載のスクランブル方式にて作成された信号を受信し、上記第1及び第2のデータと上記識別信号を検出して上記受信した信号のデスクランブルを行うようにしたスクランブル信号の受信装置。

発明の詳細な説明

以下の順序で本発明を説明する。

A　産業上の利用分野
B　発明の概要
C　従来の技術
D　発明が解決しようとする課題
E　課題を解決するための手段
F　作用
G　実施例
H　発明の効果

A　産業上の利用分野

本発明は、例えばテレビジョン信号を通信衛星を用いて送信する場合に使用されるスクランブル方式及びスクランブル信号の受信装置に関する。

B　発明の概要

本発明はスクランブル方式及びスクランブル信号の受信装置に関し、複数のデータの一つを用いてスクランブルした信号と、複数のデータと、ス

クランブルに用いられたデータの識別信号を送付することによって盗視聴を困難にすると共に、正規の受信装置では正常な受信を容易に行うことができるようにしたものである。

C　従来の技術

例えば通信衛星を用いてテレビジョン信号の送信を行う場合に、非契約者の盗視聴を禁止する目的で信号をスクランブルすることが考えられている。

その場合に、映像信号のスクランブルについては、例えば特開昭60－256286～8 号公報に示されるような、いわゆるラインシャフリングの技術が提案されている。

D　発明が解決しようとする課題

ところが、上述のように単にスクランブルのみを行っているのでは、これが無断で解読されて比較的容易に盗視聴されてしまうおそれがある。

そこでスクランブルのキー信号（ＳＤＡ）を時々刻々に変化させると共に、このキー信号をスクランブルされた信号と共に送信することが考えられ、さらにこのキー信号にもスクランブルを行ってこのキー信号をデスクランブルするデータも共に送信することが考えられた。これによればスクランブルの無断解読を相当に困難にすることができる。

しかしながらこのような方式を採用した場合に、上述のキー信号のスクランブルは、一般に任意のデータを初期値としたＭ系列等によるランダム信号を加算することによって行われている。その場合にＭ系列は完全なランダムではなく、周期性を持つために長期の観測によって解読が可能となる。

これに対して初期値のデータを時々刻々に変化させることが考えられるが、このようなデータは既に定められいる信号フォーマットの一部を使って伝送されるために常時伝送することはできず、また伝送された初期値データの切替を同期して行うことも容易ではなく、複雑な構成が必要になるなどの問題が生じた。

この出願はこのような点に鑑みてなされたもので、無断解読を極めて困難にすると共に、正規の受信装置では簡単な構成で正常な受信を容易に行うことができるようにしたものである。

E　課題を解決するための手段

本発明による第１の手段は、第１及び第２のデータ（キー信号K_3, K_4）のいずれか一方に基づいてスクランブル（回路(2)(5)）された信号と、上記第１及び第２のデータと、上記スクランブルされた信号が上記第１及び第２のデータのいずれに基づいているかを示す識別信号（発生回路(12)）とを送付するようにしたスクランブル方式である。

第２の手段は、第１及び第２のデータが交互（スイッチ(11)）に伝送され、かつ伝送される毎にそれぞれ異なる値（発生回路(7)）とされた上記第１の手段記載のスクランブル方式である。

第３の手段は、上記第１の手段記載のスクランブル方式にて作成された信号を受信し、上記第１及び第２のデータと上記識別信号を検出（メモリ(37)及び発生回路(45)）して上記受信した信号のデスクランブル（回路(22)(25)）を行うようにしたスクランブル信号の受信装置である。

F　作用

これによれば、複数のデータとスクランブルに用いられたデータの識別信号とが送付されるので、これらを総て解読して盗視聴を行うことが極めて困難になる一方、正規の受信は容易に行うことができ、簡単な構成で良好なスクランブル信号の送信及び受信を行うことができる。

G　実施例

第１図は送信から受信までのシステム構成を示し、図中(100)は送信側の装置、(200)は受信側の装置をそれぞれ全体として示している。

この図において、(1)は映像信号の入力端子であって、この入力端子(1)からの映像信号が上述のラインシャフリング等のスクランブル回路(2)に供給され、スクランブルされた映像信号が送信回路(3)

に供給される。また(4)は音声信号の入力端子であって、この音声信号は例えば48kHz でサンプリングされ16ビットで量子化されたＰＣＭ音声信号が供給される。この入力端子(4)からの音声信号がスクランブル回路(5)に供給されて、任意のビット反転等のスクランブルが行われ、このスクランブルされた音声信号が多重化回路(6)を通じて送信回路(3)に供給される。

さらに(7)はキー信号発生回路であって、この発生回路(7)からの時々刻々変化される所定のキー信号K_3が映像信号のスクランブル用のデータ（ＳＤＡ）としてスクランブル回路(2)に供給される。それと共にこのキー信号K_3(＝ＳＤＡ）が加算器（イクスクルーシブオア回路）(8)に供給されて、任意のビット反転等のスクランブルが行われ、このスクランブルされたキー信号K_3が多重化回路(6)に供給される。

また発生回路(7)からのキー信号K_4, K_3がそれぞれＭ系列等のランダム信号発生回路(9)(10)に初期値として供給され、これらの発生回路(9)(10)からのランダム信号がスイッチ(11)で選択されて、音声信号のスクランブル回路(5)及び加算器(8)に供給される。なおキー信号K_3, K_4はスイッチ(11)で選択されていない間に順次値が変更される。これによって音声信号及びキー信号K_3のスクランブルが行われる。

さらにスイッチ(11)の切替が切替信号発生回路(12)からの信号で制御されると共に、この切替状態を示すフラグ（識別信号）が多重化回路(6)に供給される。なおこの切替は後述するキー信号K_3, K_4の伝送に対して余裕を持った間隔で行われる。

また(13)はそれぞれ情報データの発生手段であって、例えばコンピュータからなるこの発生手段(13)では、チャンネル番号等の放送データ、各契約者の加入者番号及び契約チャンネル番号等の個別情報を含む加入者データ（受信登録番号）、改ざん防止用ＩＤ、誤り訂正コード等が発生される。この発生手段 (13)からの情報データが情報信号列形成回路(14)に供給される。さらに上述の発生回路(7)からのキー信号K_4, K_2及び後述のK_2, K_1が形成回路(14)に供給される。

そしてこの形成回路(14)では、例えば次に述べるような２つのフォーマットで情報信号列が形成される。すなわち第２図Ａは共通情報信号列のフォーマットを示し、時系列の先頭（左）側から例えば８ビットの後続が共通情報であることを示すヘッダＩＤ、それぞれ16ビットのキー信号K_1, K_2、それぞれ32ビットのキー信号K_3, K_4、４ビットの改ざん防止用ＩＤ、４ビットのチャンネル番号等が設けられ、末尾に24ビットの誤り訂正コードが設けられて全体が 256ビットにされている。また同図Ｂは個別情報信号列のフォーマットを示し、同じく時系列の先頭（左）側から例えば８ビットの後続が個別情報であることを示すヘッダＩＤ、22ビットの加入者番号、４ビットの改ざん防止ＩＤ、192ビットの各契約者個別情報等が設けられ、末尾に24ビットの誤り訂正コードが設けられて全体が256 ビットにされている。

この共通情報信号列及び個別情報信号列がそれぞれ加算器（イクスクルーシブオア回路）(15)(16)に供給される。さらに発生回路(7)からのキー信号K_1がランダム信号発生回路(17)に初期値として供給され、この発生回路(17)からのランダム信号が加算器(15)(16)に供給される。この加算器(16)からの信号が加算器(18)に供給されると共に、発生回路(7)からのキー信号K_2がランダム信号発生回路(19)に初期値として供給され、この発生回路(19)からのランダム信号が加算器(18)に供給される。

これによって共通情報信号列にはキー信号K_1によるスクランブルが行われ、個別情報信号列にはキー信号K_1及びK_2によるスクランブルが行われる。なお実際には、共通情報信号列ではヘッダとキー信号K_1を除くキー信号K_2以降にキー信号K_1によるスクランブルが行われ、個別情報信号列ではヘッダを除く部分にキー信号K_1及びK_2によるスクランブルが行われている。またこれらのキー信号K_1及びK_2は例えば５秒ごとに順次値が変化されている。

これらのスクランブルされた共通情報信号列及

び個別情報信号列が多重化回路(20)に供給され、例えば個別情報信号列が9回に共通情報信号列が1回の割合で、時分割多重化される。この多重化された信号が多重化回路(6)に供給される。

そしてこの多重化回路(6)では、例えば次に述べたような多重化が行われる。すなわちこの装置においては、ＰＣＭ音声信号はいわゆる放送衛星におけるＢモード音声に準拠した形式で伝送が行われている。そこで第3図は1.0s周期で伝送される1フレームのビットインターリーブマトリクスを示しており、このマトリクスは32行64列で構成される。ここで第1列，第2列はフレーム同期、音声信号のモード等を示す制御符号及びレンジビットのエリアとされ、続く第3列～第50列がＰＣＭ音声信号のエリアとされる。さらに第58列～第64列が誤り訂正コードのエリアとされると共に、これらの間の第51列～第57列はＢモード音声では独立データエリアとされている。

従って上述の多重化回路(6)においてはこの第51列～第57列のエリアにスクランブルされたキー信号K_s、スイッチ(11)の切替状態を示すフラグ及び共通情報信号列または個別情報信号列を多重化することができる。なお共通情報信号列及び個別情報信号列は、例えば各フレームに8ビットずつ伝送され、全体は32フレームかけて伝送される。そして上述のようにスクランブルされた映像信号と、スクランブル及び多重化された音声信号が送信回路(3)に供給され、例えば通信衛星（図示せず）を用いて受信側の装置(200)に伝送される。

そこでこの受信側の装置(200)において、まず受信回路(21)で受信された映像信号がデスクランブル回路(22)に供給され、上述のラインシャフリングが元に戻されて出力端子(23)に取出される。また受信回路(21)で受信された音声信号が分離回路(24)を通じてデスクランブル回路(25)に供給され、任意のビット反転等が元に戻されて出力端子(26)に取出される。

さらに分離回路(24)にて、キー信号K_sに相当する信号が分離され、この信号が減算器（イクスクルーシブオア回路）(27)に供給されて、任意のビット反転等のデスクランブルが行われる。このデスクランブルによって復元されたキー信号K_s（＝ＳＤＡ）がデスクランブル回路(22)に供給される。

また分離回路(24)にて上述の共通情報信号列及び個別情報信号列に相当する信号が分離され、この信号が減算器(28)とキー信号K_1のメモリ(29)に供給される。それと共に分離回路(24)からの信号がヘッダ検出及びタイミング発生回路(30)に供給され、この発生回路(30)からの共通情報のヘッダＩＤが検出された直後のキー信号K_1の期間に相当する信号がメモリ(29)に供給されて、キー信号K_1がメモリ(29)に書込まれる。さらにこのメモリ(29)に書込まれたキー信号K_1がランダム信号発生回路(31)に初期値として供給されると共に、発生回路(30)からの共通情報のヘッダＩＤが検出されたときのキー信号K_2以降の期間及び個別情報のヘッダＩＤが検出されたときの加入者番号以降の期間に相当する信号が発生回路(31)に供給され、この期間に発生されたランダム信号が減算器(28)に供給される。これによって共通情報信号列のキー信号K_2以降の信号のデスクランブルが行われる。

この減算器(28)からの信号が減算器(32)とキー信号K_2のメモリ(33)に供給される。それと共に発生回路(30)からの共通情報のヘッダＩＤが検出された後のキー信号K_2の期間に相当する信号がメモリ(33)に供給されて、キー信号K_2がメモリ(33)に書込まれる。このメモリ(33)に書込まれたキー信号K_2がランダム信号発生回路(34)に初期値として供給されると共に、発生回路(30)からの個別情報のヘッダＩＤが検出されたときの加入者番号以降の期間に相当する信号が発生回路(34)に供給され、この期間に発生されたランダム信号が減算器(32)に供給される。これによって個別情報信号列の加入者番号以降の信号のデスクランブルが行われる。

この減算器(32)からの信号がデータラッチ及び誤り訂正の回路(メモリ)(35)に供給される。一方発生回路(30)からの信号がメモリ制御回路(36)に供

給され、この制御回路(36)からの信号が回路(35)に供給される。これによって、上述のキー信号K_3,K_4、改ざん防止ＩＤ、チャンネル番号、加入者番号、改ざん防止ＩＤ、各契約者個別情報等のデータがそれぞれ回路(35)にラッチされる。

さらにこの回路(35)にて各情報信号列の末尾の誤り訂正コードを用いてデータの誤り訂正が行われる。そしてこの誤り訂正が終了し、データの誤りが無くなったときにそれを示す信号が制御回路(36)に供給され、この制御回路(36)からの信号がメモリ(37)に供給されて、回路(35)にラッチされた各データがメモリ(37)に転送される。

これによって各データがメモリ(37)に書込まれる。そこでこれらのデータに対して、まず加入者番号が発生回路(30)からの所定のタイミングでオーソライズ回路(38)に読出される。一方このオーソライズ回路(38)には受信装置(200)ごとに独立に設けられたデコーダ識別番号（登録番号）がその記憶手段(39)から供給され、この識別番号と上述の加入者番号（受信登録番号）とが比較され、これらが一致したときに以降の各契約者個別情報が有効とされて、ここに設けられた契約チャンネル番号等の情報が抽出保存される。そして共通情報信号列中のチャンネル番号と契約チャンネル番号とが一致したときに、デスクランブル動作の承認が行われる。またメモリ(37)の共通情報信号列のデータと個別情報信号列のデータのそれぞれに設けられた改ざん防止ＩＤが発生回路(30)からのタイミングで不一致検出回路(40)に読出され、不一致が検出されたときにメモリ(37)の内容がリセットされて全チャンネルが未契約の状態となるようにされる。

そして上述のデスクランブル動作の承認が行われたときは、メモリ(37)からのキー信号K_1,K_2がそれぞれランダム信号発生回路(41)(42)に初期値として供給され、また分離回路(24)からのフレーム同期信号が検出回路(43)で検出されて発生回路(41)(42)に供給される。これによって発生されたランダム信号がスイッチ(44)で選択されてデスクランブル回路(25)、減算器(27)に供給されると共に、分離回路(24)からのスイッチの切替状態を示すフラグ（識別信号）が切替信号発生回路(45)に供給され、この発生回路(45)からの信号でスイッチ(44)の切替が制御される。

このようにして受信された映像信号及びＰＣＭ音声信号のデスクランブルが行われる。

そしてさらにこの装置においては、送信側でキー信号K_2,K_4によるランダム信号が切替られてスクランブルが行われると共に、この切替を示すフラグ（識別信号）がキー信号K_3,K_4等と共に送信される。一方受信側では、キー信号K_3,K_4が検出されてランダム信号が発生されると共に、切替を示すフラグが検出され、このフラグに応じてランダム信号が切替られ、これによって信号のデスクランブル動作が行われる。

すなわち上述の装置において、異なる初期値によるＭ系列信号が切替えて用いられることによって、Ｍ系列によるランダム信号の周期性が除かれ、その解読が極めて困難にされる。一方正規の装置ではキー信号K_3,K_4と識別信号が送付されることによってデスクランブルを極めて容易に行うことができる。

なお識別信号（フラグ）は例えば１ビットのデータであるので、上述の共通情報及び個別情報のフォーマット以外の任意のデータエリアで伝送することができ、常時伝送を行うことによって極めて良好な切替を行うことができる。

またキー信号K_3,K_4はスイッチ(11)(44)で選択されていない期間に順次変更されることによって、無断解読が一層困難になるようにすることができるものである。

従って上述の装置によれば、複数のデータとスクランブルに用いられたデータの識別信号とが送付されるので、これらを総て解読して盗視聴を行うことが極めて困難になる一方、正規の受信は容易に行うことができ、簡単な構成で良好なスクランブル信号の送信及び受信を行うことができるものである。

なお上述の装置において、デスクランブルの承認を個別情報信号列をデスクランブルするデータ

が検出されるまで禁止することによって誤動作の発生を良好に防止している。

またキー信号K₁でスクランブルされた情報の中に個別情報信号列のスクランブルのキー信号K₂を設けることによって個別情報信号列の機密性を極めて高くしている。

さらに改ざん防止ＩＤを設けることによって盗視聴を良好に禁止している。

またデスクランブルされたデータを一旦ラッチし、誤りが無いときのみメモリに転送することによって誤動作のおそれを大幅に減少させている。

H　発明の効果

この発明によれば、複数のデータとスクランブルに用いられたデータの識別信号とが送付されるので、これらを総て解読して盗視聴を行うことが極めて困難になる一方、正規の受信は容易に行うことができ、簡単な構成で良好なスクランブル信号の送信及び受信を行うことができるようになった。

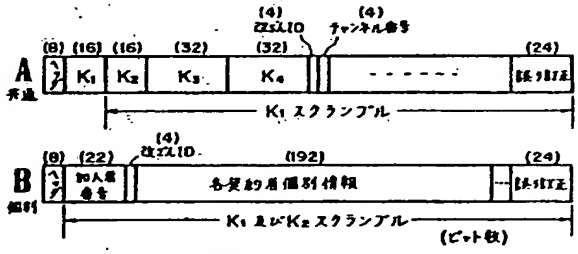
受信装置である。

代　理　人　　松　隈　秀　盛

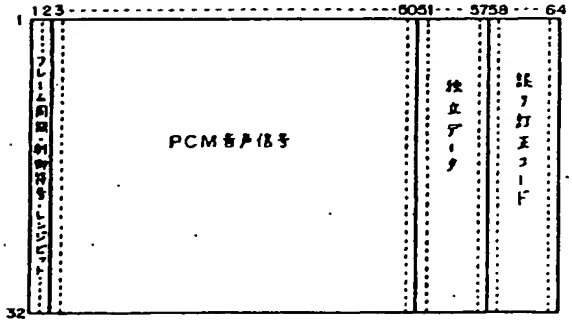
図面の簡単な説明

第１図は本発明によるスクランブル信号の受信装置を含む全体のシステムの一例の構成図、第２図は伝送される情報信号列のフォーマットを示す線図、第３図はＰＣＭ音声信号のビットインターリーブマトリクスを示す線図である。

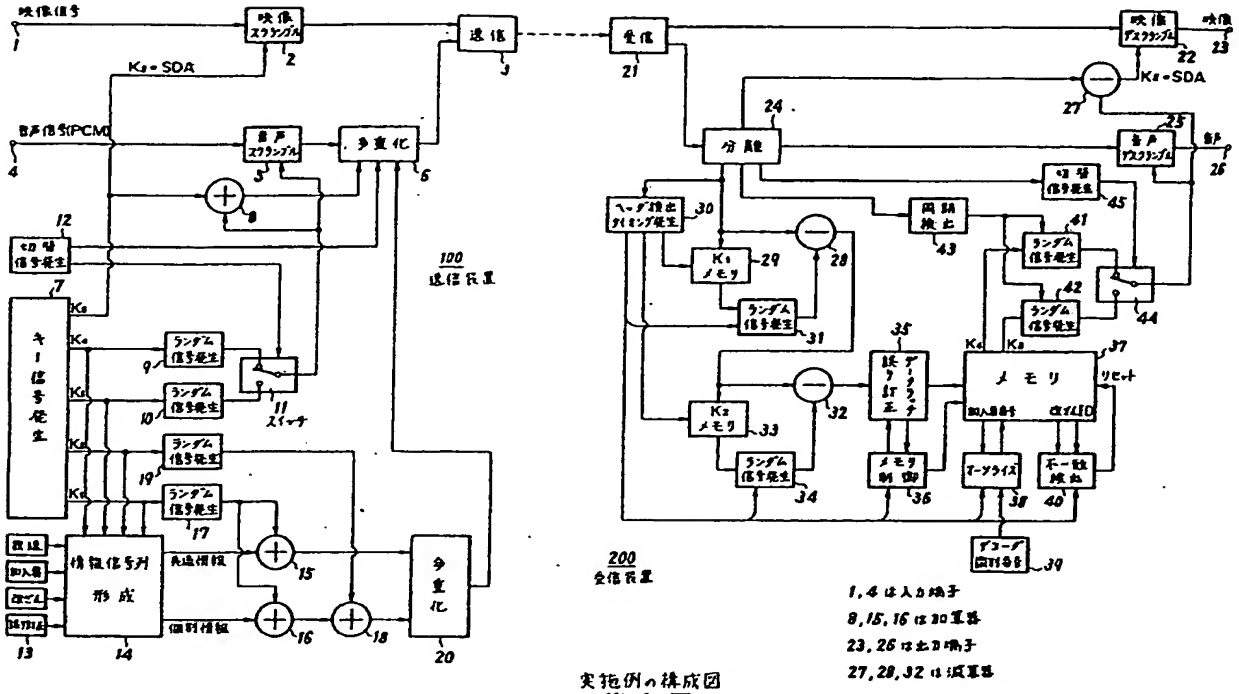
(1)(4)は入力端子、(2)(5)はスクランブル回路、(3)は送信回路、(6)(20)は多重化回路、(7)はキー信号発生回路、(8)(15)(16)(18)は加算器、(9)(10)(17)(19)(31)(34)(41)(42)はランダム信号発生回路、(11)(44)はスイッチ、(12)(45)は切替信号発生回路、(13)は情報データ発生回路、(14)は情報信号列形成回路、(21)は受信回路、(22)(25)はデスクランブル回路、(23)(26)は出力端子、(24)は分離回路、(27)(28)(32)は減算器、(29)(33)(37)はメモリ、(30)はヘッダ検出及びタイミング発生回路、(35)はデータラッチ及び誤り訂正回路、(36)はメモリ制御回路、(38)はオーソライズ回路、(39)は識別番号の記憶手段、(40)は不一致検出回路、(43)は同期検出回路、(100)は送信装置、(200)は



情報信号列フォーマット
第２図



ビットインターリーアマトリクス
第３図


映像信号
音声信号(PCM)
Ks=SDA
100
送信装置
200
受信装置
キー信号発生
情報信号形成
多重化
分離
メモリ
1,4は入力端子
8,15,16は加算器
23,26は出力端子
27,28,32は減算器

実施例の構成図
第 1 図